UNITED STATES DISTRICT COURT

for the

Western District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

INFORMATION ASSOCIATED WITH MITCHELL.BROS.INC@GMAIL.COM THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE LLC

Case No. 1:18-mj-100-DLH

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. Section 1341	Frauds and swindles
18 U.S.C. Section 1343	Fraud by wire, radio, or television
18 U.S.C. Section 1030(a)(4)	Unauthorized access in the furtherance of fraud

The application is based on these facts:

See attached affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Corey S. Zachman, FBI Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: September 7, 2018

Judge's signature

City and state: Asheville, North Carolina

Dennis L. Howell, U.S. Magistrate Judge

Printed name and title

Western District of North Carolina

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA
ASHEVILLE DIVISION

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH MITCHELL.BROS.INC@GMAIL.COM THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE LLC	Case No. 1:18-MJ-100-DLH Filed Under Seal

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Corey S. Zachman, after being duly sworn, depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI). I have been so employed since February 2013. I currently conduct national security investigations for the Charlotte, North Carolina, Division of the FBI. Prior to my employment with the FBI, and starting in 2008, I was a Federal Agent with the Air Force Office of Special Investigations, where I conducted national security investigations for the Department of Defense. From 2005 to 2008, I worked as an attorney practicing primarily in the areas of business and construction litigation, and I was licensed to practice in the State of Utah and the United States Court of Appeals for the Tenth Circuit. I have been trained by the FBI in the preparation, presentation, and service of criminal complaints and arrest and search warrants, and have been involved in the investigation of numerous types of offenses against the United States.

2. I submit this affidavit in support of a warrant to search contents and records associated with the Gmail account mitchell.bros.inc@gmail.com, hereinafter the SUBJECT ACCOUNT, which is located on computer systems in the control of Google LLC The domain to be searched is more particularly described in Attachment A.

3. As set forth in this Affidavit, your Affiant has probable cause to believe that the registrant(s) and user(s) of the SUBJECT ACCOUNT has committed violations of, among other

statutes, Title 18, United States Code, Section 1341 (Frauds and swindles) and Title 18, United States Code, Section 1343 (Fraud by wire, radio, or television), and Title 18, United States Code, section 1030(a)(4) (Computer fraud). As set forth herein, the unknown user(s) of the SUBJECT ACCOUNT has initiated, or attempted to initiate, multiple fraudulent transactions to swindle manipulate entities and individuals into shipping stolen computer hardware to locations in West Africa.

4. Title 18, United States Code, Section 1341 provides, "Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses . . . for the purpose of executing such scheme or artifice . . . deposits or cause[s] to be deposited any matter or thing whatever to be sent or delivered by any private or commercial interstate carrier . . . [shall be guilty of a crime]." 18 U.S.C. § 1341.

5. Title 18, United States Code, Section 1343 provides, "Whoever, having devised any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses...transmits or causes to be transmitted by means of wire...any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice...[shall be guilty of a crime]." 18 U.S.C. 1343.

6. Title 18, United States Code, Section 1030(a) provides, in relevant part, that whoever "Knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value . . . shall be guilty of an offense against the United States." 18 U.S.C. § 1030(a)(4).

7. The facts set forth below are based upon my personal observations, on reports and information provided to me by other law enforcement officials, and on records obtained by the FBI. This affidavit is intended only to show that there is probable cause for the issuance of the requested

search warrant, and it does not purport to set forth all of my knowledge of or investigation into this matter.

Jurisdiction & Venue

8. The Stored Communications Act allows a governmental entity to obtain contents of wire or electronic communications in a remote computing service, as well as records concerning electronic communications or a remote computing service, by securing "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction." *See* 18 U.S.C. §§ 2703(a), (b)(1)(A), (C)(1)(A). The SCA defines the term "court of competent jurisdiction" to include "a district court of the United States [that] has jurisdiction over the offense being investigated." 18 U.S.C. Section 2711(3)(A)(i). The SCA therefore overrides the traditional venue requirements set forth for a search warrant in Federal Rule of Criminal Procedure 41(b). *See In re Info. Associated with @gmail.com*, Case No. 16-mj-00757 (BAH), 2017 U.S. Dist. LEXIS 130153, *61 (D.D.C. July 31, 2017) (holding that, by adding the "court of competent jurisdiction" language to the SCA, "Congress ensured that an SCA warrant was not bound by Rule 41(b)'s venue restrictions.").

9. This Court is "a district court of the United States [that] has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). This investigation relates to violations of the federal criminal laws, and this Court has original, exclusive subject matter jurisdiction over "all offenses against the laws of the United States." 18 U.S.C. § 3231. Moreover, the Western District of North Carolina—and, more particularly, the Asheville division thereof—is "a district where the offense was committed." Fed. R. Crim. P. 18. While this Affidavit focuses primarily on certain episodes in which the suspected fraudsters used re-shippers located in Maryland and California as conduits for their offense conduct, your Affiant has also been in contact with re-shippers within the

Western District of North Carolina who have been contacted and used by the targets of this investigation in furtherance of their fraud. For example, in or about September 2017, Steve Guffey, President of Chamad Warehouse/Distribution, received a call from a person claiming to be "David Johnson." Johnson informed Guffey that Guffey would be receiving a pallet of computers at his warehouse in Marion, North Carolina. Once the computers arrived, Johnson would contact Guffey with instructions on repackaging and reshipping the computers. The computers expected to arrive in Marion, North Carolina, were the same computers the individuals attempted to purchase from Microsoft, as detailed in the Probable Cause section below.

Probable Cause

10. On or about September 18, 2017, John Roth, World Wide Business Consultant—Microsoft Business & Education Sales Team, received an online request for information about the purchase of Microsoft Surface Devices. The request purported to come from Kary L. Washington, Procurement Specialist, University of Maryland Baltimore County (UMBC). Over the course of approximately a month, Roth coordinated with the individual claiming to be Washington for an increase in UMBC's credit with Microsoft and for UMBC's purchase of 40 Microsoft Surface computers totaling $71,402.40. The individual claiming to be Washington provided the billing address of UMBC, 1000 Hilltop Circle, Room 923, Baltimore, MD 21250, which is the actual address for UMBC. However, the individual claiming to be Washington requested that the computers themselves be shipped to a different address: University of Maryland—Baltimore County, IT & Service Center Building, 8220 Patuxent Range Road, Jessup, Maryland 20794.

11. Prior to the shipment of the Surface computers, Microsoft became suspicious of the order and contacted UMBC's procurement office. UMBC's procurement office had no knowledge of the purchase, and there was no person employed at the office by the name of Kary Washington.

12. Greg Ginther, Microsoft Retail Loss Prevention Manager, contacted the FBI and provided the foregoing information on the attempted purchase of Surface laptops. A check of the shipping address provided by the individual purporting to be Washington showed that the address actually belonged to "Coleman Worldwide Moving," a moving company that also provides package forwarding/re-shipping services. Coleman Worldwide Moving also goes by "Coleman World Group," and will be referred to hereafter simply as "Coleman."

13. Based on the information received from Microsoft, a law enforcement officer interviewed Rick DiSanti, General Manager for Coleman, who stated that on or about November 10, 2017, he had received an e-mail from a person purporting to be Scott Engle, President/CEO of Freight Logistics, Inc., informing DiSanti that DiSanti would receive a delivery of approximately 30 boxes via UPS in the near future. Freight Logistics appears to be a legitimate company, and a person by the name of Scott Engle does appear to be employed by that company. However, the person claiming to be Scott Engle used the e-mail address scott.engle@ship-fli.com, while later inquiries by law enforcement revealed that genuine Freight Logistics e-mail addresses end in @shipfli.com (with no hyphen). Based on your Affiant's training and experience, the differences between those e-mail addresses reflects a practice known as "spoofing." As commonly understood, "spoofing" is the forgery of an e-mail address or e-mail header information to make the communication appear to come from a reputable organization or source.

14. On or about November 10, 2017, the boxes mentioned by the person claiming to be Engle arrived, and the packing slip showed that the boxes contained computers which had been ordered from Dell and apparently sold to "UMBC-UNIVERSITY OF MARYLAND BALT COUNTY/ACCOUNTS PAYABLE/1000 HILLTOP CIR/BALTIMORE, MD." That was the same billing information that "Kary Washington" provided to Microsoft in the course of the

attempted fraud previously discussed. At the same time, the shipping address was "UMBC-UNIV MARYLAND BALT COUNTY/RICK DISANTI/8220 PATUXENT RANGE RD/IT & AUXILLARY SERVICE/JESSUP, MD US 20794," which is the address for Coleman and which was again consistent with the attempted fraud previously detected by Microsoft. DiSanti thought it was strange that UMBC would ship to Coleman, considering that UMBC was located approximately five (5) miles from Coleman.

15. The person claiming to be Engle requested via e-mail that DiSanti "[k]indly repack them [the Dell computers] as usual" and then prepare them for shipment. The person claiming to be Engle provided a Bill of Lading, and Coleman repackaged the computers and prepared them for shipment. A company called Daylight Transport picked up the computers for shipment to Cargo Solution, 18521 Gale Ave., City of Industry, CA 91748. All of this took place before law enforcement interviewed DiSanti.

16. On or about November 27, 2017, after law enforcement interviewed DiSanti, DiSanti received another e-mail from the person claiming to be Engle, with Freight Logistics. The new e-mail stated that "[t]here will be another delivery of 30 boxes via UPS tomorrow Tuesday, 11/28/2017. Kindly repack as usual and let me know as soon as it is ready."

17. The packing slip that arrived at Coleman with the first 15 computers indicated that the purchaser had ordered 30 Lenovo NoteBook TP P51 16G 512 W10P computers (hereafter, the COMPUTERS), and that all 30 had shipped. The packing slip further displayed ship-to addresses of UNIVERSITY OF MARYLAND ATTN Rick DiSanti, 8220 Patuxent Range Road (the address for Coleman). DiSanti reported the arrival of the first 15 boxes to the FBI.

18. On November 28, 2017, an FBI agent contacted Mallela Ralliford, Contract Administrator, UMBC. Ralliford confirmed that all large (and legitimate) purchases by the university,

such as the purchase of 30 Notebook computers, would have been processed by the procurement office. But she had no record of 30 NoteBook computers purchased from Lenovo, and she was aware of someone using UMBC's name to purchase computers in the past.

19. On November 29, 2017, the remaining 15 Lenovo NoteBook computers arrived at the Coleman facility at 8220 Patuxent Range Road. At this time, based on information provided by DiSanti, all the computers were located at the Coleman facility. The computers arrived at the Coleman facility in two separate boxes, each of which contained fifteen small computer boxes. The targets expected Coleman to re-pack and re-ship the COMPUTERS to another location. The re-shipping addresses were provided by the person claiming to be Engle on or about December 04, 2017.

20. On or about December 04, 2017, Coleman received a Bill of Lading from the person claiming to be Engle showing that the COMPUTERS would be shipped from Coleman to Cargo Solution Inc., 18521 Gale Ave., City of Industry, California 91748. A check of this address disclosed it was the address for Zheijiang Sunmarr International Transportation Company Limited, a warehouse/shipping company, referred to hereafter as "Sunmarr." The Gale Avenue location of Sunmarr was run by Roger Zhang.

21. Prior to the arrival of the COMPUTERS, a law enforcement officer interviewed Roger Zhang, who stated that he had been doing business with Cargo Solutions since approximately 2015. His point of contact for the account was a man named Azeez Adekunle. Approximately every two weeks, Zhang would receive one to two pallets of computers or computer equipment that he would repackage and ship to Nigeria for Adekunle.

22. Zhang had been contacted in the past by law enforcement asking about Cargo Solutions and their shipments to Nigeria. After this initial interview, Zhang reached out to Adekunle and asked him why law enforcement would be interested in his business. Adekunle responded that it

was an online business where he purchased computer equipment in the US and sold it in Nigeria, but did not offer any additional information.

23. Adekunle and Zhang would communicate via e-mail, with Adekunle using the e-mail address info@fastfreightglobal.com. Adekunle would e-mail Zhang, using that e-mail address, and inform him that pallets of computers would be arriving at the Sunmarr warehouse. Adekunle would often attach the Bill of Lading for the shipments, so Zhang would know what to expect, and request that Zhang take pictures of the shipment when it arrived and send the pictures to Adekunle using the e-mail address info@fastfreightglobal.com. Zhang would also e-mail invoices for shipments to Adekunle at the e-mail address info@fastfreightglobal.com.

24. On or about January 31, 2018 your Affiant conducted an open source domain search on info@fastfreightglobal.com, using a "Domain Whois" search. The Domain Whois search disclosed that fastfreightglobal.com was hosted on the servers of U.S. company Liquid Web Inc. Your Affiant also confirmed that Liquid Web hosts the e-mail exchange for fastfreightglobal.com and info@fastfreightglobal.com.

25. On or about June 1, 2018, in response to a search warrant for records related to fastfreightglobal.com, the FBI received records from Liquid Web Inc. related to fastfreightglobal.com and the e-mail addresses associated with fastfreightglobal.com, to include info@fastfreightglobal.com. A review of those e-mails disclosed that between approximately May 2017 and May 2018 the e-mail address info@fastfreightglobal.com would receive e-mails from, mitchell.bros.inc@gmail.com, the SUBJECT ACCOUNT, titled "Pickup." The body of the e-mail would contain a name, often it would be the name SCOTT ENGLE, an address, and a general list of items to be picked up.

26. The SUBJECT ACCOUNT, mitchell.bros.inc@gmail.com, comes from a person purporting to be G.C.. Open source research disclosed Mitchell Brothers Truck Line Inc. appears to

be a legitimate company based in Vancouver, Washington of which G.C. was the owner/president of the company until his death on or about October 9, 2013. The e-mail domain used by Mitchell Brothers from the inception of the company has always been @mitchell-bros.com and never mitchell.bros.inc@gmail.com.

27. On or about February 23, 2018, an e-mail was sent from the person purporting to be G.C., using e-mail address mitchell.bros.inc@gmail.com, to info@fastfreightglobal.com. The subject of the e-mail was "Pick Up (MD) and the body of the e-mail was as follows:

> Scott Engle
> Advance Relocation Systems
> 11500 Crossroads Circle
> Middle River, MD 21220
> 301-241-7009
> No. of Skids: 1 – Weight: 670 lbs
> No. of boxes: 6 – Weight: 183 lbs
> Content: Laptops

28. That e-mail was then forwarded to DOF Cargo out of Miami Florida to pickup the cargo, repackage it, and then ship it on to Johannesburg, South Africa. On or about February 27, 2018, using the same e-mail chain, the person using info@fastfreightglobal.com contacts DOF Cargo to inquire about the status of the laptops, and when they will be shipped from DOF Cargo's warehouse. DOF Cargo notifies the user of info@fastfreightglobal.com that DOF Cargo "...received a call from another vendor and [a] detective came to the office. Apparently there is more than one case about this and they are investigating the situation. As of right now they will take possession of the cargo and we are not allowed to do anything with it. From what they told me this is part of a group of individuals that do this all the time." The user of info@fastfreightglobal.com then forwarded that e-mail on to the mitchell.bros.inc@gmail.com e-mail address. The person purporting to be G.C.

continued to send e-mails with pickup locations for additional laptops and computer equipment using the mitchell.bros.inc@gmail.com e-mail address.

29. The above stated facts are consistent with subject's practice to use one spoofed e-mail domain, or e-mail address, such as the @umbc.edu address, to deceive the manufacturer into shipping to the first re-shipper. Adekunle's co-conspirators then use additional spoofed e-mail domains, or e-mail addresses, to direct the first re-shipper to forward the stolen property to Zhang. Finally, Adekunle uses an e-mail address, or e-mail addresses, from the @fastfreightglobal.com domain to direct Zhang to re-ship the stolen property to West Africa. Because Adekunle appears to have communicated with SUBJECT ACCOUNT on a regular basis, and with respect to shipments of stolen computers/computer equipment, your Affiant believes that the SUBJECT ACCOUNT is a sham account created and operated solely for the purpose of perpetrating the fraud.

30. Moreover, based on your Affiant's training, experience, consultation with other agents, and participation in other investigations involving persons who conspire to commit complex crimes, your Affiant asserts that the commissioners of cyber frauds often use e-mail communications to conduct planning, to stay in contact with associates, and to keep records of their illegal activities. Specifically, similar investigations have shown e-mail communications between conspirators to provide contact information, to share or store flight itineraries, and to transmit banking and payment information, or invoices. Similar investigations have also shown that commissioners of cyber frauds will use e-mail accounts to maintain records reflecting the names, nicknames, addresses, e-mail addresses, and telephone numbers of both current and past associates. Often, such information is contained in multiple e-mail/online accounts, such that viewing it individually makes the information appear innocuous, however, when viewed collectively, the information provides a clearer picture of networks and associates. These sorts of records and information are all frequently contained within

e-mail communications, and they are therefore often maintained indefinitely within a user's e-mail account.

31. In addition to records and information related to other shipments of stolen goods directed by Fast Freight Global and Adekunle, your Affiant submits that there is probable cause to believe that records and information of the types outlined in Paragraph 30 will be contained within the SUBJECT ACCOUNT.

Technical Background

32. Through training and experience, your Affiant has learned that Google LLC is a company making its headquarters at 1600 Amphitheatre Parkway, Mountain View, CA 94043, provides a variety of on-line services, including electronic mail or "e-mail" access, to the public. Google allows subscribers to obtain e-mail accounts at the domain name "gmail.com," like the account listed in **Attachment A**. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers and servers of Google are likely to contain stored electronic communications (including retrieved and un-retrieved e-mail for Google subscribers) and information concerning subscribers and their use of Google services, such as account information, e-mail transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

33. In addition, a Google subscriber can store on servers maintained or owned by Google other files related or in addition to the e-mail, such as contact lists, address books, calendar data, pictures other than images attached to e-mails. Through training and experience, your Affiant is aware that evidence of who was using an e-mail account can frequently be found in these related files.

34. In my training and experience, e-mail providers generally ask their subscribers to provide certain personal identifying information when registering for an e-mail account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying customers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

35. In my training and experience, e-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

36. In my training and experience, in some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services,

as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

37. This application seeks a warrant to search all responsive records and information under the control of Google, a provider subject to the jurisdiction of this court, regardless of where Google has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Google's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.

38. In general, an e-mail that is sent to a Google LLC subscriber is stored in the subscriber's "mail-box" on Google LLC servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Google LLC servers indefinitely.

39. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the internet to Google LLC servers, and then transmitted to its end destination. Google LLC often saves a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from the Google LLC server, the e-mail can remain on the system indefinitely.

40. Affiant anticipates executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. Section 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) and Federal Rule of Criminal Procedure 41, by using the warrant to require Google LLC to disclose to the government copies of the records and other information (including the content of communications) particularly described in Attachment B.

Conclusion

41. The evidence believed to be located within the SUBJECT ACCOUNT is listed in **Attachment B** of this Affidavit, which is incorporated by reference as if fully set forth herein, and is believed to be contained on servers and digital storage media maintained by and under the control of Google LLC. Your Affiant requests authority to search for and seize such material.

42. This application seeks a warrant to search all responsive records and information under the control of Google, a provider subject to the jurisdiction of this court, regardless of where Google has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers is such communication, record, or other information is with Google's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.

43. Your Affiant is aware that many providers of digital services, such as e-mail accounts, have staff members who work shifts other than traditional business hours. Such staff members may at times be responsible for compiling materials responsive to search warrants. Therefore, your Affiant requests that this warrant be executable at any time of the day or night, as that may be more convenient for the responding party.

44. Pursuant to 18 U.S.C. §2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

45. This is an ongoing investigation. Due to the volatile nature of digital data, your Affiant is aware that if notified of the existence of a search warrant, many individuals will take steps to delete other materials that may have evidentiary value pertaining to the criminal violations described herein.

Therefore, your Affiant requests this Court also issue an order to Google that precludes Google from notifying the subscriber(s) of the SUBJECT ACCOUNT that a search warrant has been authorized or that an investigation is underway. Your Affiant is also aware that closing an account can indicate to a subscriber that the subscriber is under investigation. Therefore, your Affiant further requests that this Court order Google to refrain from unilaterally closing the SUBJECT ACCOUNT to preserve the integrity of the investigation and prevent destruction of potential evidence.

46. Your Affiant further requests that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court, or until such time as legal proceedings, if any, related to this investigation are instituted and the subject of charges, if any, appears in Court.

47. In consideration of the foregoing, your Affiant respectfully requests that this Court issue a search warrant for the search of the Google account mitchell.bros.inc@gmail.com more specifically described in **Attachment A** which is incorporated by reference as if fully set forth herein, authorizing the seizure and search of the items described in **Attachment B** herein.

Sworn to under penalty of perjury:

Date 9-7-18

Corey S. Zachman
Special Agent, Federal Bureau of Investigation

Sworn to and subscribed before me this the 7th day of August 2018 in Asheville, North Carolina:

The Hon. Dennis L. Howell
United States Magistrate Judge for the
Western District of North Carolina

ATTACHMENT A

Property to Be Searched

I. Service of Warrant and Copying of Computer Files by ISP

A. The officer executing this warrant shall effect service by any lawful method including faxing the warrant (with the consent of Google LLC) to the offices of Google LLC at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

B. The officer executing this warrant shall permit Google LLC, as custodian of the computer files described in Section II below, to locate the files, copy them onto a removable electronic storage media or print them out as paper copies (or use a different copying method if specified in Section II below), and deliver the copies to the officer, who need not be present during this process at the location specified in the warrant.

II. Description of Account to be Searched

Information associated with the following accounts:

mitchell.bros.inc@gmail.com

that is stored at premises controlled by Google LLC, a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A from Inception to Present:

a. All records, files, and other information (including data and the content of electronic communications or contained in "draft" or "trash" Gmail folders) for the Google Services of Account Activity, Drivesync Invite, Gauss, Gmail, Google App Engine Admin Console, Google Calendar, Google Docs, Google Drive, Google Maps Engine, Google Talk, Knowledge Search, Lso Provider, Omaha, Web History, YouTube, and iGoogle associated with the account username;

b. The contents of all text messages, voicemails, recorded calls, emails, and chat messages associated with the account, including stored or preserved copies of chat logs, emails sent to and from the account, draft communications, the source and destination addresses associated with each communication, the date and time at which each communication was sent, and the size and length of each communication;

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, login IP addresses associated with session times and dates, account status,

alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. All device information associated with the account;

e. All location history associated with the account;

f. All search and browsing history associated with the account;

g. All Google Bookmarks;

h. All voice and audio activity associated with the account;

i. Any account trustees or managers associated with the account;

j. The types of service utilized;

k. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

l. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

m. For all Google accounts that are linked to any of the accounts listed in Attachment A by cookies, creation IP address, recovery email address, or telephone number, provide:

1. Names (including subscriber names, user names, and screen names);

2. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses);

3. Local and long distance telephone connection records;

4. Records of session times and durations and IP history log;

5. Length of service (including start date) and types of service utilized;

6. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"),

Mobile Equipment Identifier ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), MSISDN, International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Station Equipment Identities ("IMEI"));

7. Other subscriber numbers or identities (including temporarily assigned network addresses and registration IP addresses (including carrier grade natting addresses or ports)); and

8. Means and source of payment for such service (including any credit card or bank account number) and billing records.

The provider is hereby ordered to disclose the above information to the government within **14 DAYS** of the issuance of this warrant.

II. Information to be seized by the Government

All information described above, in Section I, that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. §§ 1341, 1343, and/or 1030(a)(4), or other federal criminal statutes, involving mitchell.bros.inc@gmail.com and occurring after January 2017, including without limitation, for each account or identifier listed on Attachment A, information pertaining to the following matters:

A. Evidence indicating how and when the domain account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the domain account owner;

B. Evidence indicating the domain account owner's state of mind as it relates to the crime under investigation;

C. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

D. The identity of the person(s) who communicated with the user ID about matters relating to wire fraud or other frauds and/or swindles.